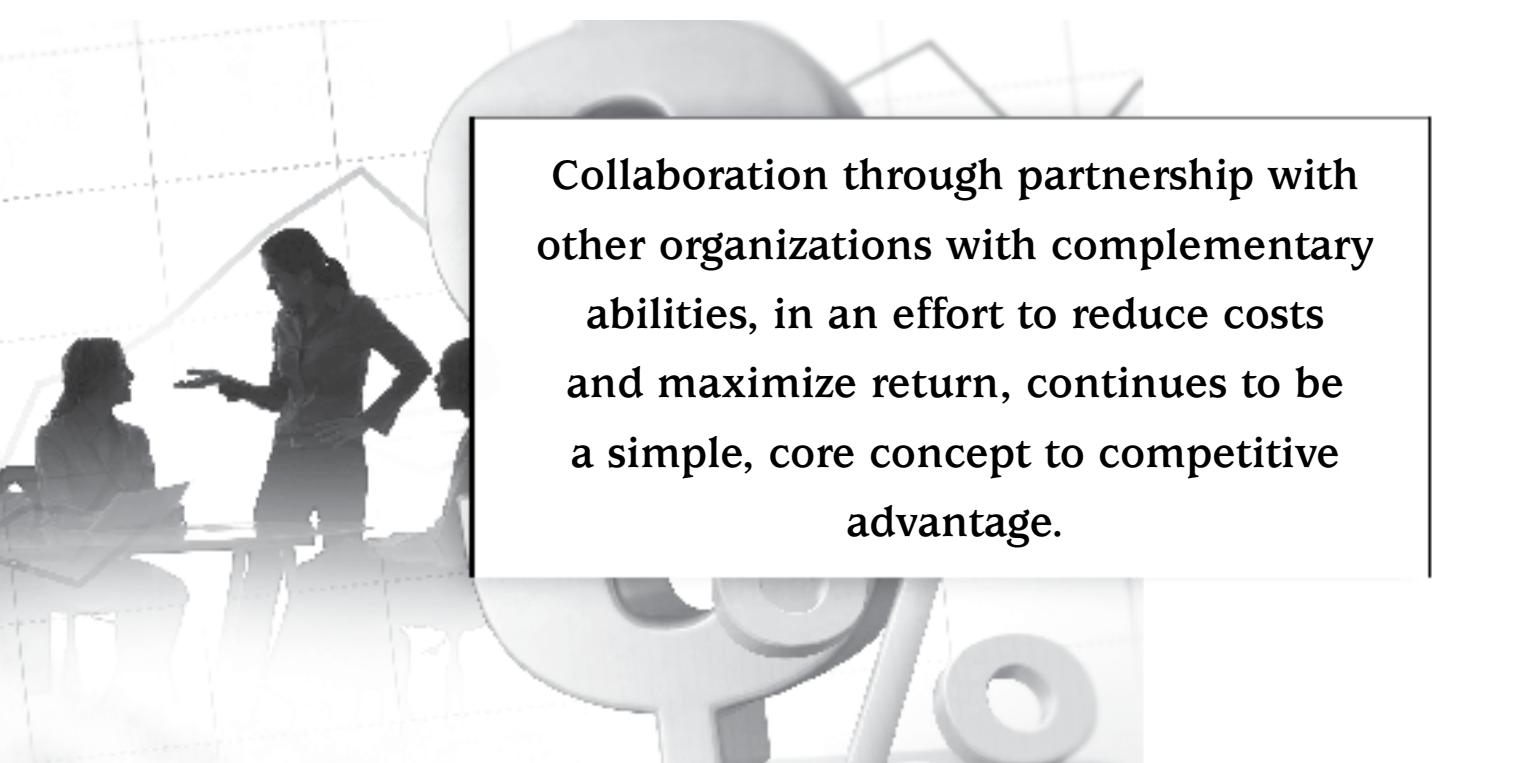


Secure Information Sharing: Part I

Shaping Industry Interaction

Paul Grant ■ Jeff Nigriny



Collaboration through partnership with other organizations with complementary abilities, in an effort to reduce costs and maximize return, continues to be a simple, core concept to competitive advantage.

Along-standing imperative to share information drives the Department of Defense and its partners to create and improve the defense information-sharing environment where the power of information ensures mission success. DoD's information-sharing strategy centers on enhancing the Department's efficiency and effectiveness through net-centric operations that deliver an agile enterprise empowered by access to and sharing of timely and trusted information. The ultimate goal: collaboration among those involved.

Collaboration takes on many different forms, from design to sourcing to teaming during operational phases of complex programs. In general, it means working together to produce a common result. A major target for this vision is DoD's supply chain, which is one of the most—if not the most—complicated supply chains in the world. With

a supply chain the size and scope of DoD's, collaboration can drive even minute improvements that bring impressive aggregate returns.

Information sharing can lead to efficiency no matter where it is done; supply chains simply have some additional nuances in contracting and in how risk is shared. Overall though, collaboration through partnership with other organizations with complementary abilities, in an effort to reduce costs and maximize return, continues to be a simple, core concept to competitive advantage.

To define and establish best practices for secure information sharing that enables collaboration delivering advantage, DoD has been an active participant in the Trans-global Secure Collaborative Program (TSCP) for almost a half decade. The progress toward specifications needed for collaboration in the unique environments in this industry has helped all participants better position capabilities to share sensitive, controlled information while improving such information assurance requirements as export controls and privacy protection.

Grant is the information assurance executive for the Department of Defense. **Nigriny** is outreach director for the Transglobal Secure Collaborative Program and chief security officer for Exostar, the leading provider of secure collaboration and integrated supply-chain solutions to the aerospace and defense industry.

New Supply Chain Paradigm Drives Call for Secure Information Sharing

The evolution of defense contracting is a well-documented subject that spans many decades. The most recent breakthrough is illustrated by the much-documented Joint Strike Fighter with its unprecedented need for collaboration among multiple nations and partners. Viewed as one of the earliest examples of modern DoD contracting, the JSF program was DoD's primary focus in affordable next-generation strike aircraft weapon systems for the Navy, Air Force, Marines, and U.S. allies. Lockheed Martin Corporation (LMCO) was selected as the prime contractor and teamed with Northrop Grumman and BAE Systems. Sourcing of the aircraft engines was orchestrated as a competition between Pratt and Whitney and a team of Rolls-Royce and GE.

The collaboration among such a diverse design and development team is complex, but not as complex as the requirements of those organizations in charge of financing. The United States and United Kingdom are *collaborative partners*; others, including Denmark, Norway, The Netherlands, Canada, and Italy, are viewed as *cooperative partners*. Additionally, Singapore, Turkey, and Israel are foreign military sales participants in the system development and demonstration phase of the program.

This model was a major catalyst in the creation of the TSCP, the only government-industry partnership of its kind, which was chartered with defining the specifications for identity federation, online collaboration, and digital rights management-related technologies in mission-critical aerospace and defense (A&D) environments. At the time the JSF was conceptualized, it quickly became apparent that all mission partners in the community were addressing common issues, and that coming together to work on resolutions would allow all to achieve goals much more quickly and cost effectively.

As concerns of data leakage, intellectual property protection, and export control compliance began to rise, the TSCP began its mission to establish an industry approach to protecting sensitive information based on interoperable trust mechanisms.

The TSCP's framework for secure information sharing is threefold, and it addresses DoD's top concerns:

- **Identity management:** Who is the person I'm sharing data with?
- **Access control and privilege management:** What am I going to let that person see and gain access to?
- **Information management and resource management marking:** What data do I have?

In 2005, the program began to deliver on individual components of the framework that could be used to demonstrate the value of TSCP and show real capability in the

context of defense programs. That direction resulted in the formation of the first three capabilities: a public key infrastructure bridge, in production today as CertiPath (www.certipath.com); a secure e-mail implementation, Secure E-mail version 1.0, which was released to the public domain in October 2007; and document sharing with identity federation (DSIF) capability, currently a technology proof of concept.

Tackling E-Mail

Secure e-mail was one of the first mechanisms identified as a "killer app" (essential core application) for information sharing. Much data leakage occurs as a result of indiscriminate sharing of sensitive data over e-mail when organizations lack common security tools and processes.

Fearing that e-mail could be a problem application for the TSCP, many organizations tried for a long time to avoid using e-mail to share sensitive information, especially externally.

Teaming with the TSCP, DoD has recently completed successful technical testing with its infrastructure of a secure e-mail implementation. It is now anticipated that *For Official Use Only* and *Sensitive But Unclassified* materials will be transmitted using the application.

DoD hasn't been the only government body to benefit. The British Ministry of Defence will also be using secure e-mail to send U.K.-restricted e-mail over the Internet. The progress made in the ability to share e-mail securely is a beginning. However, e-mail is at best a rudimentary tool in terms of providing the collaborative functionality required in today's global business environments. The next level is online collaboration where revision and iteration history are inherent and access control is set with fine-grained permission. This is being tackled now through the TSCP's document-sharing and identity federation (DSIF) initiatives.

The Bigger Challenge: Document Sharing

DSIF is about having data ontology and a set of consolidated policies that allow for the flow of sensitive data from one network to the next with the minimum amount of local configuration and the maximum amount of security. Not having to create accounts and issue credentials to partners is one of the rare examples of something that saves money and improves security at the same time.

A field test of the TSCP's work on defining specifications for DSIF in A&D environments is currently under way using a Microsoft® SharePoint server (a collaborative tool) at LMCO on projects where LMCO and BAE Systems are working as partners. This real-world implementation illustrates two major advantages of DSIF: First, there are no accounts for the BAE Systems users at LMCO, and there are no credentials that need to be



The Transglobal Secure Collaborative Program is a rare example of a trust fabric and federation that has come together to figure out how best to implement a complex set of relationships in a digital setting.

managed and maintained by LMCO on behalf of BAE Systems teammates. Authentication is accomplished through identity federation policy and technology. Second, the “quality” of the authentication the BAE Systems users perform when they wish to access the LMCO SharePoint instance (i.e., username and password or digital certificates) is provided to LMCO so SharePoint can provide more or less access to information based purely on the authentication method. This is a relative first in unclassified space and was accomplished by the technical people at TSCP. These requirements and the proof of concept were presented to Microsoft in September 2007 to be considered for inclusion in Windows® Version 7/“Vienna,” the next version of the Windows operating system.

The Next Frontiers

The next two initiatives DoD will address with the TSCP are intellectual property protection and export control inside a product life-cycle-management environment, and then the same intellectual property protection and export control in real-time collaboration (for example, online whiteboarding—a capability that enables geographically separated people who are conferenced together to annotate and draw collaboratively on shared images or slides appearing on the screen).

A key enabler for these next two initiatives is a technology and policy concept called DRM—digital rights management. DRM provides the mechanism by which trust can be extended from the data owner to a single data recipient, even at a remote organization.

DRM solves the concerns attached to sending a sensitive piece of information to someone at a different organization. Among the most common concerns are fears that a

mail relay somewhere will get a copy of the information or that the administrator of the servers at the recipient’s network will realize and exploit the black market value of the data. We don’t feel we can rely on having our intended recipient alone receive the data. And even if that were not an issue, we would still be worried about what might happen to the information tomorrow or the next day while it sits on a “foreign” hard drive.

The idea that we can control data at a granular enough level to define the who, when, and how of receipt, has the potential to give us confidence that our data won’t be accessed inappropriately or in a manner inconsistent with our wishes as the data owner—the aim of information security in the first place.

DoD and TSCP: Defining Best Practices in Information Sharing

The TSCP’s mission—to find a way for employees, contractors, and suppliers to securely access internal data as well as that of foreign governments and suppliers—continues to be important to DoD as an enabler of increased information sharing.

The provision of a framework for collaboration and sharing has been hugely beneficial for DoD, increasing trust and confidence. Along with other partners, DoD is spending resources on collaboration, identity management, data-sharing management, and common business languages.

DoD’s intention is to continue and expand upon guidance on better and compliant use of data, which will aid the implementation of DoD policy in areas such as the unique identification of tangible assets and the achievement of net-centricity, with inherent data segregation

management and federated, collaborative identity and access management.

Participation in the TSCP provides multiple benefits in support of DoD's overall vision of the move to net-centric operations:

- The re-use of data-sharing models and tools across programs
- The definition of a common baseline of organizational and individual security on which trust can be formed
- Collaborative toolsets that will interoperate with partners, suppliers, and customers.

Specific to the A&D supply chain, participants gain:

- Compliance with export control regulations in a more predictable and controlled manner
- The ability to meet the emerging requirements of identity assurance—a major new DoD initiative.

In addition to the work with the TSCP, DoD is progressing on separate but completely inter-related areas of responsibility, including unique asset identification, export-control compliance, information assurance, and activity-based costing. It is mutually beneficial to use the TSCP to achieve collaborative progress in these areas, across defense industries, thereby benefiting each other.

DoD will maintain its current level of effort in participation and membership with the TSCP. In the near future, it hopes to recognize some of the potential benefits for major acquisition programs to become early adopters of TSCP output, including JSF, DD(X) [*next-generation multi-mission surface combatants tailored for land attack and littoral dominance*], and Alliance Ground Surveillance.

Looking Ahead

The TSCP is a rare example of a trust fabric and federation that has come together to figure out how best to implement a complex set of relationships in a digital setting. Lessons learned have come not only from the technical output and proofs of concept but also from the very way in which the TSCP has organized itself to work. Significant effort has gone into defining the ways of working to ensure that everyone's needs are met. TSCP represents not only best practices in secure collaboration but some of the very best thinking and practical implementations in teaming.

In Parts II and III, we will examine the collaboration efforts behind the TSCP and the implementations of the TSCP's specifications for information sharing among member organizations for major programs.

The authors welcome comments and questions and can be contacted at paul.grant@osd.mil and jeff.nigriny@certipath.com.

Project Management *continued from page 36*

priorities, it's up to the project manager to keep their attention on the right project deliverables and deadlines. However, hovering around people and looking over their shoulders won't help and will probably hinder. Periodic status reports should be sufficient.

18. Using "outsiders" correctly is a team multiplier.

Whether it is quality assurance, configuration management, testing, matrixed personnel, or even upper management, use non-team members in tasks where their talents can fill a need. Ask for help when you need it, and apply the help where it does the most good.

19. Focus on the important areas, but don't ignore the rest.

It is the project manager who is ultimately responsible for everything. Put the emphasis where it is required, but leave the detailed activities to the appropriate team members. It is the manager's job to oversee and monitor. It may mean giving encouragement, correcting people, or jumping in to help at times, but that can't be all of the time or in all areas. Just don't forget the "outliers"—those things on the edges that don't require constant attention.

20. Expectations should be high for your self and your people, and realistic for the stakeholders.

People live up to—or down to—expectations. If you set high but reachable goals and share those expectations with the team members, they can attain them. At the same time, setting realistic expectations with the boss and/or the customer is critical. Don't over-promise.

There are many more axioms that could be added to the list. In fact, I'll add one as a bonus:

21. Don't lose your sense of humor.

Step back and look. There is plenty that is funny about what we do, how we go about things, the situations, and the people. Sometimes if you don't laugh, you might have to cry, and laughing is better.

Project management is certainly a mix of art, science, and luck. However, good luck seems to gravitate to the well-prepared person who works hard at his or her craft. Following the guidelines in this article will help you to be more prepared, and then there's a much better chance the good luck you need for success in your project will come your way.

The author welcomes comments and questions and can be contacted at rwturk@aol.com or wayne.turk@sussconsulting.com.